A CLIENT-SERVER ARCHITECTURE SUPPORTING MLS INTEROPERABILITY WITH COTS COMPONENTS

J. N. Froscher
M. H. Kang

Naval Research Laboratory
Information Technology Division
Washington, D.C. 20375

ABSTRACT

A major challenge facing the MLS community is to find ways to provide the information and connectivity that DoD users demand without either imposing unacceptable security risks or requiring expensive hardware and software that fails to mesh with commercial off-the-shelf (COTS) applications. This paper proposes, very briefly, an architecture that meets these goals using only a small number of relatively simple, low cost, high assurance components in combination with a preponderance of unmodified COTS hardware, operating systems and applications.

INTRODUCTION

The computing landscape has changed dramatically over the past decade, evolving from a world of stand-alone computers whose users occasionally exchange email to a globally networked computing environment in which resources anywhere can be accessed anytime by almost anyone. Recognizing this shift, the Joint Security Commission (JSC) [1] challenged the MLS community to find better ways to protect national security resources: "Our paradigm for managing security must also shift from developing security for each individual application, system, and network to developing security for subscribers within the worldwide utility."

As new computing paradigms appear, such as distributed object-oriented computing, DoD organizations must be able to share information, integrate new technologies into their information systems, and, at the same time, protect their information and guarantee their operational advantage. Commercial and government enterprises have turned to client-server architectures to achieve global interoperability. For many critical functions, however, DoD continues to rely on legacy systems (stovepipe, single-purpose, inflexible, isolated systems) whose design and purpose never addressed the need for global interoperability and information sharing.

We propose a security architecture that can be applied to a system or to a globally distributed confederation of heterogeneous components to enable reliable, secure information sharing among organizations operating over a wide range of security levels. First, we mention some techniques for inter-enclave information sharing that require only a few relatively simple security-critical components, yet can make information available securely to the widest community of MLS users. We propose three principles for future MLS architectures and summarize an architecture based on them that responds to the JSC's challenge. We then provide details on the client side and the server side of our proposed architecture and describe the other components required for the comprehensive architecture. Finally, we assess how our architecture supports both security requirements and needs for interoperability, support for legacy systems, and incentives to increase information sharing.

SIMPLE TECHNIQUES FOR INFORMATION SHARING

Some techniques that facilitate inter-enclave information sharing through the use of relatively simple security critical components are:

- Replication of information from low to high systems, as demonstrated in SINTRA prototypes [2] using COTS replication servers in conjunction with the NRL Pump [3], a reliable, one-way flow device.
- Higher level user access to lower level resources on demand, without the use of special purpose trusted operating systems, as demonstrated by the Australian Starlight Interactive Link [4] facility at JWID '96.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **1997**	2. REPORT TYPE	3. DATES COVERED **00-00-1997 to 00-00-1997**

4. TITLE AND SUBTITLE **A Client-Server Architecture Supporting MLS Interoperability with COTS Components**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Research Laboratory,Information Technology Division,4555 Overlook Avenue, SW,Washington,DC,20375**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**4**	

- Assurance of information privacy, integrity, and authenticity through judicious use of cryptographic techniques.

High assurance downgrading is presently needed in some situations, often because low sensitivity data have been imported into a high enclave and need to be exported to a lower level. Simple, high assurance components to achieve this function have yet to be demonstrated. In the long term, it will be preferable to collect and store such data at its correct sensitivity level.

PRINCIPLES AND ARCHITECTURE

Our response to the JSC's challenge is based on three principles:

- *Security engineering in the large:* Security must be designed into the global infrastructure. High assurance components are needed for strong separation, while low assurance security mechanisms can be used for weak separation.
- *Separation of concerns:* Security concerns should be focused on separate components, permitting maximum use of COTS components to meet other functional requirements.
- *Minimize MLS access to shared resources:* Accesses to a single shared resource from processes at different security levels is the major source of residual vulnerabilities in MLS systems. Physical separation and data replication can provide the same function but with much stronger, more effective protection.

On this basis, we propose to build a secure heterogeneous distributed system from multiple single-level COTS products and appropriate simple, special-purpose security components.

There are two parts to our solution: client and server. The distributed SINTRA DBMS and the NRL Pump are primarily server side solutions. The Australian Starlight Interactive Link (IL) technology represents a promising client side solution, although general high-assurance approaches for handling downgrading need attention. This approach reduces cost by encouraging the use of COTS products, provides a path for legacy systems to migrate to new technologies, and promotes information sharing while maintaining the security and autonomy of organizations.

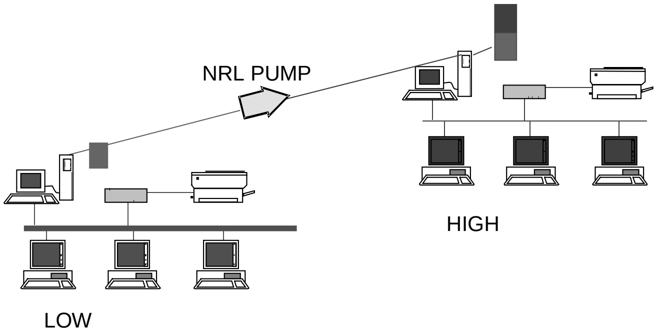

Figure 1. Server Side Solution: SINTRA with Pump

A SERVER-SIDE SOLUTION

The server-side solution is based on the following observations:

1. MLS security can be achieved by separation of computing resources, and
2. Replication of low information to high systems and applications makes low information available to high users.

When the information is propagated from lower to higher level systems, we need a one-way communication component that assures that this communication not only preserves the secure information flow but also guarantees reliability, fairness, availability, and performance. The NRL Pump is a device that balances the above requirements. The server-side solution is shown in Figure 1.

A CLIENT-SIDE SOLUTION

Our client-side solution is based on the following observations:

1. Security can be achieved by separation of computing resources, and
2. When lower level information or services are needed by higher level users, they can be provided by establishing a separate connection to lower level systems.

The Starlight Interactive Link is a device developed by the Australian Defence Science and Technology Organization (DSTO) that enables the user of a COTS X Windows workstation in a secure enclave to redirect the output of his keyboard to login to lower level servers to browse, send messages or have data sent to the higher enclave for future analysis. In other words, a high level user can establish simultaneous connections to systems at many lower security levels through a Starlight-enabled workstation. The client-side solution is shown in Figure 2.

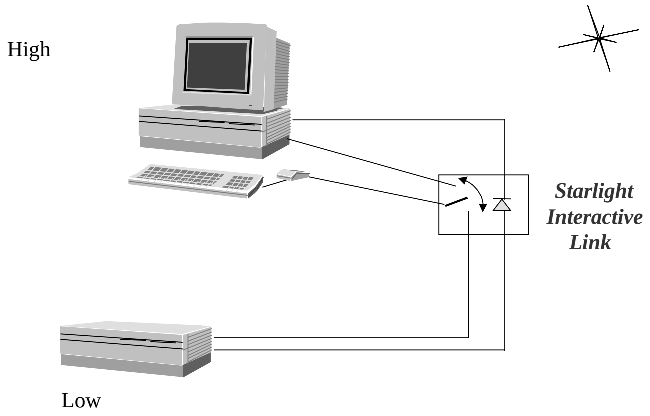

Figure 2. Client Side Solution: Starlight Interactive Link

COMPREHENSIVE SECURITY ARCHITECTURE

The security architecture can be achieved by combining the server-side and client-side solutions, and adding a few other components [5]. The other components are needed to assure privacy, authenticity, and integrity of messages in the network and to permit downgrading. The architecture for two security levels shown in Figure 3 can be extended easily to handle three or more levels.

ASSESSMENT

Our architecture meets the security requirements as follows:

- ***Information flow from low to high system.*** If lower level information needs to be sent to higher level systems: (1) the information is encrypted and authenticated (if necessary), (2) it is sent to the Pump through a network, (3) it is delivered to the final destination, and (4) it is decrypted and verified (if necessary). Note that steps (3) and (4) can be reversed depending on system requirements.

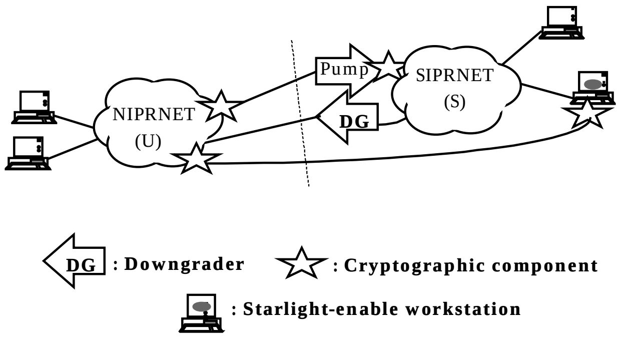

Figure 3. Comprehensive Architecture

- ***Privacy, integrity, authenticity of information.*** If information travels through an unprotected portion of a network and the information needs protection, then cryptographic components can be used.
- ***Higher level users may need to access lower level resources.*** If higher level users need to access lower level information that has not been replicated to a higher level system, then the high user can login to a lower level system via Starlight Interactive Link. Again, if the network is not protected and the information requires protection, then cryptographic techniques should be used.
- ***Availability of resources.*** No single technique can solve this problem, although the fault-tolerant community uses replication to increase availability. Our proposed architecture uses replication as a way to share lower level information with higher level processes/users. We believe that minimal, but cleverly engineered use of replication can also help achieve the goals of availability, performance, and sharing.
- ***Downgrading.*** If there is a need to downgrade information, then a downgrader should be used (see figure 8). If the downgraded information is still at a higher security level than the security level of the unprotected portion of the network, then cryptographic techniques should be used.

Additional benefits of our approach include:

- ***Reduced cost.*** The overall cost of our approach will be much lower than that of the naive extensions of the traditional MLS approach because our approach encourages the use of commercially available products.
- ***Provision of a migration path for legacy systems.*** Legacy systems can participate in new federations without jeopardizing security because these systems are isolated by security critical components.
- ***Provision of a migration path to new technologies.*** When new products or technologies are available, an organization can incorporate these in the federation without affecting other organization/systems. This is true because systems from different organizations are strongly separated by security critical components.
- ***Promotion of sharing, security, and autonomy.*** Since the security of our proposed approach is flexible and easy to understand, it encourages organizations to participate in federations while retaining full control of their own systems. Each organization can decide which critical components are needed, depending on their own security and functionality needs.

REFERENCES

[1] Joint Security Commission, "Redefining Security--A Report to the Secretary of Defense and the Director of Central Intelligence," 28 Feb. 1994.

[2] Froscher, J. N., M. H. Kang, J. P. McDermott, O. Costich, and C. E. Landwehr, "A Practical Approach to High Assurance Multilevel Secure Computing Service," *Proc. Tenth Annual Computer Security Applications Conference*, Orlando, FL, Dec., 1994.

[3] Kang, M. H., Moskowitz, I. S. and Lee, D. C., “A Network Pump” *IEEE Transaction on Software Engineering, vol. 22*, no. 5, May, 1996.

[4] Anderson, M., North, C., Griffin, R., Yesberg, J., and Yiu, K., “Starlight; Interactive link,” *Proc. Twelfth Annual Computer Security Applications Conf.*, San Diego, CA, Dec., 1996.

[5] Kang, M. H., Froscher, J. N., and Moskowitz, I. S., “A Framework for MLS Interoperability,” *Proceedings of IEEE HASE Workshop*, Oct. 1996.